

## LISTING OF THE CLAIMS:

The following is a complete listing of all the claims in the application, with an indication of the status of each:

1-3. (Canceled).

- 1     4. (Previously Presented) A method of verifying knowledge of a secret number  
2      $s$  in a prover device by a verifier device having no knowledge of the secret  
3     number, the method comprising a zero-knowledge protocol using a  
4     Montgomery representation of numbers and Montgomery multiplication  
5     operations therein,  
6         wherein the zero knowledge protocol comprises the Fiat-Shamir  
7     protocol,  
8         the method further comprising:  
9         (i)     providing to the verifier device a value  $v = s^2$  being the  
10     Montgomery multiplication of the secret number  $s$  by itself,  
11         (ii)    computing, by the prover device, a value  $x = r \times_m r$ , where  $r$  is a  
12     random number, and transmitting the value  $x$  to the verifier device;  
13         (iii)   selecting, by the verifier device, a challenge value of  $e$  from a set  
14      $\{0, 1\}$  and transmitting the challenge value to the prover device;  
15         (iv)    computing, by the prover device, a value  $y = r \times_m s^e$ , and  
16     transmitting the value  $y$  to the verifier device; and

17 (v) the verifier device checking an authenticity of the prover's response  
18 according to the values  $x$ ,  $y$  and  $v$  previously received and according to the  
19 challenge value  $e$ .

1 5. (Previously Presented) The method of claim 4 wherein the step of checking  
2 the authenticity of the prover's response comprises the steps of:

3 for a challenge value of  $e = 1$ , computing the values of  $y \cdot x_m y$  and  $v \cdot x_m x$   
4 and checking that they are the same; or

5 for a challenge value of  $e = 0$ , computing the value of  $y \cdot x_m y$  and  
6 checking that it is the same as the previously received value of  $x$ .

1 6. (Previously Presented) The method of claim 4 further including the steps of  
2 repeating steps (ii) to (v) for a number of consecutive rounds to confirm the  
3 authenticity of the prover's response.

1 7. (Previously Presented) The method of claim 4 in which the secret number  
2  $s$  is a Montgomery representation of another number  $s'$  known in the prover  
3 device domain but not in the verifier device domain, further including the  
4 step of computing, by the prover device, the value of  $s$  from  $s'$  according to  $s$   
5  $= s'R \bmod n$ , where  $R > n$ , values of  $n$  and  $R$  being used by both the prover  
6 device and the verifier device.

1 8. (Previously Presented) The method of claim 4 in which the Montgomery  
2 multiplications of  $s \times_m s$ ,  $r \times_m r$ , and  $r \times_m s^e$  are carried out according to the  
3 formula  $a \times_m b = abR^{-1} \bmod n$ , where  $R > n$ , values of  $n$  and  $R$  being used by both  
4 the prover device and the verifier device.

1 9. (Previously Presented) The method of claim 5 in which the Montgomery  
2 multiplications of  $y \times_m y$  and  $s^2 \times_m x$  are carried out according to the formula  $a$   
3  $\times_m b = abR^{-1} \bmod n$ , where  $R > n$ , values of  $n$  and  $R$  being used by both the prover  
4 device and the verifier device.

1 10. (Previously Presented) The method of claim 4 in which all computations in  
2 the zero knowledge protocol are performed using Montgomery representation  
3 of numbers and using Montgomery multiplication operations.

11 - 30. (Canceled)